Notice of Allowability	Application No.	Applicant(s)	
	10/582,803	FUTA ET AL.	
	Examiner	Art Unit	
	MINH DIEU NGUYEN	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/18/2099*.

2. ☒ The allowed claim(s) is/are *1,4-15 and 18-21*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *9/4/09* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mark D. Pratt on 9/4/09.

2. The application has been amended as follows:

Claim 1

(Currently Amended) A prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising:

a prime storage unit storing the known prime q;

a management information storage unit storing unique management information;

a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information;

a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N using the read prime q and the generated random information R, according to N = 2 x random information R x prime q ÷ 1;

a primality testing unit operable to test primality of the calculated prime candidate N according to the Pocklington's primality test; and

an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined,

wherein said random information generation unit further includes:

a reading subunit operable to read the unique management information from the management information storage unit;

a random number calculation subunit operable to calculate a random number r;

a combining subunit operable to make a combination of the read unique management information and the ~~generated~~ calculated random number r; and

a computation subunit operable to compute the random information R based on the combination, and

wherein the computation subunit computes the random information R by applving an injection function to the combination.

Claim 18

(Currently Amended) A key issuing system including a terminal and a key issuing server apparatus for generating and issuing a private key and a public key of RSA encryption for the terminal, wherein

the key issuing server apparatus comprises:

a prime calculation unit operable to calculate a prime N larger than a known prime q;

a public key generation unit operable to generate the public key using the

calculated prime N;

a private key generation unit operable to generate the private key using the generated public key;

a key output unit operable to output the generated private key to the terminal; and a publishing unit operable to publish the generated public key,

the prime calculation unit includes:

a prime storage subunit storing the known prime q;

a management information storage subunit storing unique management information;

a random information generation subunit operable to read the unique management information from the management information storage subunit, and generate random information R based on the read unique management information;

a candidate calculation subunit operable to read the prime q from the prime storage subunit, and calculate a prime candidate N using the read prime q and the generated random information R, according to N = 2 x random information R x prime q+l;

a primality testing subunit operable to test primality of the calculated prime candidate N;

an output subunit operable to output the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined; and

an iteration control subunit operable to control the random information generation subunit, the candidate calculation subunit, and the primality testing subunit

to iterate the generation of the random information R, the calculation of the prime candidate N, and the primality testing until the primality of the calculated prime candidate N is determined by the primality testing subunit, and

the terminal includes:

a reception unit operable to receive the private key; and

a key storage unit operable to store the received private key, wherein said random information generation subunit further includes:

a reading subunit operable to read the unique management information from the management information storage unit;

a random number calculation subunit operable to calculate a random number r;

a combining subunit operable to make a combination of the read unique management information and the ~~generated~~ calculated random number r; and

a computation subunit operable to compute the random information R based on the combination, and

wherein the computation subunit computes the random information R by applying an injection function to the combination.

Claim 20

(Currently Amended) A prime calculation method used in a prime calculating apparatus that calculates a prime candidate N larger than a known prime q and tests primality of the calculated prime candidate N, the prime calculating apparatus including:

a prime storage unit storing the known prime q; a management information storage unit storing unique management information; and a secondary information storage unit storing a predetermined verification value, the prime calculation method comprising:

a random number generation step of reading the unique management information from the management information storage unit and generating random information R based on the read unique management information;

a candidate calculation step of reading the prime q from the prime storage unit, and calculating the prime candidate N using the read prime q and the generated random information R, according to N = 2 x random information R x prime q + 1;

a primality testing step of testing primality of the calculated prime candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined,

wherein said random number generation step further includes;

a reading subunit step of reading the unique management information from the management information storage unit;

a random number calculation subunit step of calculating a random number r;

a combining subunit step of making a combination of the read unique management information and the ~~generated~~ calculated random number r; and

a computation subunit step of computing the random information R based on the combination, and

wherein the computation subunit step computes the random information R by applying an injection function to the combination, and the candidate calculation step and the primalitv testing step are performed by a program stored on a computer-readable recording medium that when executed by at least one processor causes the prime calculation apparatus to perform the candidate calculation step and the primality testing step.

Claim 21

(Currently Amended) A computer-readable recording medium storing a prime-calculation computer program, the prime-calculation computer program being used on a prime calculating apparatus that calculates a prime candidate N larger than a known prime q and tests primality of the calculated prime candidate N, the prime calculating apparatus including: a prime storage unit storing the known prime q; a management information storage unit storing unique management information, and a secondary information storage unit storing a predetermined verification value, the prime-calculation computer program comprising:

a random number generation step of reading the unique management information from the management information storage unit and generating random information R based on the read unique management information;

a candidate calculation step of reading the prime q from the prime storage unit, and calculating the prime candidate N using the read prime q and the generated random information R, according to N = 2 x random information R x prime q + 1;

a primality testing step of testing primality of the calculated prime candidate N; and

an output step of outputting the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined,

wherein said random number generation step further includes;

a reading subunit step of reading the unique management information from the management information storage unit;

a random number calculation subunit step of calculating a random number r;

a combining subunit step of making a combination of the read unique management information and the ~~generated~~ calculated random number r; and

a computation subunit step of computing the random information R based on the combination,

wherein the computation subunit step computes the random information R by applying an injection function to the combination.

Allowable Subject Matter

3. Claims 1, 4-15 and 18-21 are allowed.

4. The following is an examiner's statement of reasons for allowance: Claims 1, 4-15 and 18-21 are allowable in light of Applicant's remarks filed on 8/18/09.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

6. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2438